ABSTRACT

A network architecture allows an intermediary to inspect an encrypted data stream on a virtual private network (VPN) in a secure and trusted manner. The endpoints establish a virtual private network by negotiating a session key used to encrypt data being exchanged between them. The endpoints know the session key, but not the intermediary. To grant the intermediary trusted access to the data stream on the VPN, one endpoint securely transfers the session key to the firewall by encrypting the session key using the intermediary's public key and then signing the encrypted session key. The intermediary authenticates the signature and decrypts the session key using its own private key. If the process yields a valid key, the intermediary is assured that the session key was sent by the endpoint and was not subsequently tampered with in route. Once the session key is transferred, the firewall can decrypt and inspect the data stream on the VPN in a manner that is transparent to the endpoints.